Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 5 (2011) 539–545

Procedia Computer Science

The 8th International Conference on Mobile Web Information Systems

Security of MBAN based Health Records in Mobile Broadband Environment

Debopam Acharya[a], Vijay Kumar[b]

[a]Department of Computer Sciences, Georgia Southern University, Statesboro, GA 30460,USA
[b]School of Computing and Engineering, University of Missouri, Kansas City, MO 64110, USA

Abstract

Strong developments in mobile computing and web systems within the last decade have led to their integration in different aspects of our life. This has enabled us to explore new possibilities in the healthcare sector in the form of real time health monitoring and diagnosis systems. Mobile broadband technologies like WiMAX and LTE are being introduced at a rapid pace. This will lead to the development of healthcare systems involving round-the-clock mobile health monitoring, high volume data transmission for remote tests and diagnosis and other real time applications. There are several security issues that should be addressed to enable secured medical data transfer in a mobile broadband environment. In this work, we identify all such security issues and vulnerabilities involving transmission of medical data and propose a security scheme to address some of these issues.

Keywords: MBAN; Mobile WiMAX; Mobile Healthcare Management; EMR; EHR; Security; Location Signature;

1. Introduction

Rapid advances in mobile and wireless technologies have led to the development of smart, user preference-oriented and context-aware devices. In the near future, wireless sensors will be fully integrated in clothing, appliances, and vehicles and in every place we can imagine. An important area involving use of wireless sensors is mobile and pervasive healthcare [1]. Most of these wireless health sensors use Bluetooth wireless communication to form a personal area network. Others connect to wireless local area network and transfer data to a central device. The fractured market of wireless healthcare devices with no major standardized platform (except Bluetooth) is affecting the growth of the mobile health industry. To provide a common platform, the Federal Communications Commission (FCC) in the United States of America has recently proposed to allocate radiofrequency spectrum exclusively for medical sensors and establish service and technical rules for the operation of Medical Body Area Network (MBAN) Systems [2]. The FCC envisions that MBANs would provide a platform for wireless networking of multiple body sensors to monitor physiological data. The use of MBANs would help eliminate the need for hardwired, patient-attached cables used by current monitoring technologies. The FCC's proposal is a continuation of its efforts to satisfy the spectrum requirements of wireless medical technologies. Some of the bands proposed by FCC are 2300-2305 MHz, 2360-2400 MHz and 2400-2483.5 MHz Band. MBAN could be created through attaching multiple miniature wireless sensors on our body. These sensors would take readings of key information such as

Selection and/or peer-review under responsibility of Prof. Elhadi Shakshuki and Prof. Muhammad Younas.
doi:10.1016/j.procs.2011.07.070

temperature, pulse, blood glucose level, blood pressure, respiratory function, and a variety of other physiological metrics. These data will be wirelessly transmitted to a hub device placed at a short distance which would then relay the data to a central facility (like call center) for further processing, diagnosis and storage. Hence, increased availability and miniaturization of wireless sensors under a common platform will help the healthcare industry move out from existing wired telemedicine systems based monitoring to more advanced MBAN based mobile healthcare management (MHM).

Mobile broadband technology is currently being standardized with mobile Wireless Interoperability for Microwave Access (WiMAX) [8] already deployed in major cities. Another upcoming standard is the Long Term Evolution (LTE) [10] and efforts are on to standardize it before rolling it out to different markets by 2011-2012. The mobile WiMAX (IEEE 802.16e standard) comes from IEEE family of protocols and extends the wireless access from the Local Area Network (typically based on the IEEE 802.11 standard) to Metropolitan Area Networks (MAN) and Wide Area Networks (WAN). It uses a new physical layer radio access technology called OFDMA (Orthogonal Frequency Division Multiple Access) for uplink and downlink. The LTE defines a new physical layer radio access technology based on Orthogonal Frequency Division Multiple Access (OFDMA) for the downlink, similar in concept to the physical layer of Mobile WiMAX, but uses single Carrier Frequency Division Multiple Access (SC-FDMA) for the uplink. We argue that a MBAN created by using standardized wireless healthcare sensors together with 4G technologies like mobile WiMAX will help create a robust and efficient MHM system. To achieve this, there are several issues that should be addressed. One of the most important issues is security of health data/records collected and transmitted in the wireless environment. In this work, we identify security threats and vulnerabilities of such data in a 4G based MHM system.

The rest of the paper paper is organized as follows: Section 2 presents the architecture of MHM system. We identify and address various security/authentication threats involving such a system in section 3. Section 4 describes a possible solution to some these threats that we will address in our future work. Section 5 concludes the paper.

2. Architecture of MHM System

4G technologies have the potential to revolutionize healthcare management. We present one such MHM architecture involving 4G technologies in Fig. 1. MBAN sensors and patches can be attached to the body that collects real time physiological data. A 4G smart phone collects these data and creates an electronic healthcare record (EHR). Its transfers the EHR to a web server kept in a call centre. The call centre monitors physiological data, sends alerts if necessary and frequently multicasts context aware health education modules containing preventive healthcare techniques. The call centre may send abnormal physiological data for further tests and results are then sent to a physician for further diagnosis. The physician can diagnose current results and access patient's electronic medical record (EMR) to accurately identify the problem. The results are sent back to the patient. The patient may choose to contact the physician for an audio/video consultation. Based on the consultation, the physician may prescribe medicines with the help of an electronic prescription that can be downloaded by the patient in his/her smart phone. The patient sends the prescription to the pharmacy and pick up the drugs at a later time according to his/her convenience. This preventive action and timely consultation will be extremely beneficial to the patient, hospitals and insurance agencies [3]. If the physician diagnoses an emergency condition, he relays the message to the call centre which in turn notifies it to emergency services for prompt action. The call centre may also send alerts to patient's relatives and friends about the emergency situation.

2.1 Difference between an EHR and an EMR

It is important to distinguish between an EMR and an EHR to identify the security risks associated with them [4]. An EMR is the legal record of clinical services for patient encounters in a care delivery organization (CDO) and owned by the CDO with non-interactive patient access. This can only be accessed either by the CDO or by a medical practitioner. EHR is a subset of each CDO's EMR and owned/accessed by the patient. Also, whenever a patient collects physiological data and transfers it to a server, it is stored as an EHR. The EMR is created in a CDO.

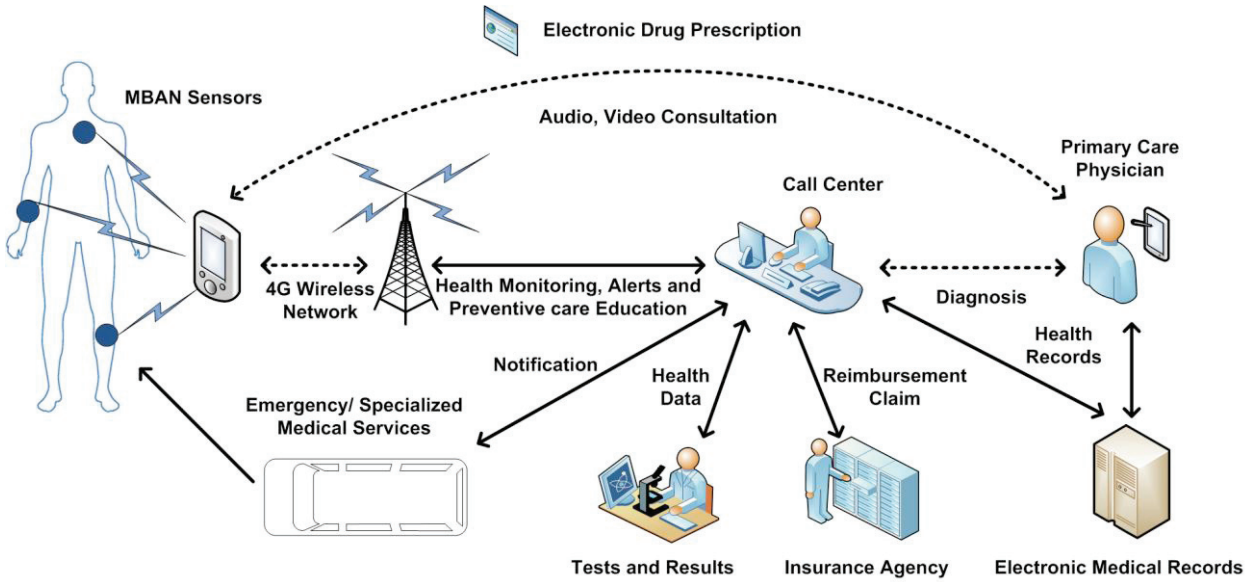

Fig. 1 Mobile Healthcare Management (MHM) Architecture

It is the source of data for the EHR. The advantage of EHR is that it can be shared and made available wherever (patients, healthcare providers, insurance, government, etc.) it is needed.

3. Security of Medical/Health Records

Security of medical/health records is a serious issue. Precisely, this involves security and privacy of EMR access by physicians or CDO and EHR access by patient using 4G wireless networks. 4G Healthcare Systems may involve medical data transmission as follows: (a) Physiological data transmission between MBAN sensors and a 4G mobile unit (MU); (b) Data transfer between MU and a web server. This will involve physiological data transmission and EHR access; (c) Data transfer from web server to Physician for diagnosis (patient's EMR access); (d) Audio/Video Consultation and electronic prescription transfer between patient and physician. (a)'s data transmission is in a MBAN and rest may involve data transmission in a 4G network. Each of these sections faces several threats and vulnerabilities as shown in Fig. 2.

3.1 Security issues in MBAN

Security attacks to health data collected in MBAN can be classified into two types: Active and Passive attacks. Active attacks are made by adversaries who have the capability to eavesdrop on medical data traffic inside MBAN. Adversaries can inject malicious messages and replay old messages. They can also set up spoof nodes in or around MBAN to become a part of the network. Unintentional flooding of connection requests by foreign nodes may also prevent the host node to connect to other nodes in the MBAN. All these are Denial of Services (DOS) attacks that not only compromise patient's private medical data but can also substitute/modify legitimate medical data with bogus messages into the network. This can lead to catastrophic consequences such as preventing notification to medical services/hospitals in case of emergency. Passive attacks are made by adversaries who only have the capability to eavesdrop on the communication inside MBAN without interfering with the functionality of it. The attackers can compromise patient's privacy by performing crypt-analytical attacks on the eavesdropped medical data or messages.

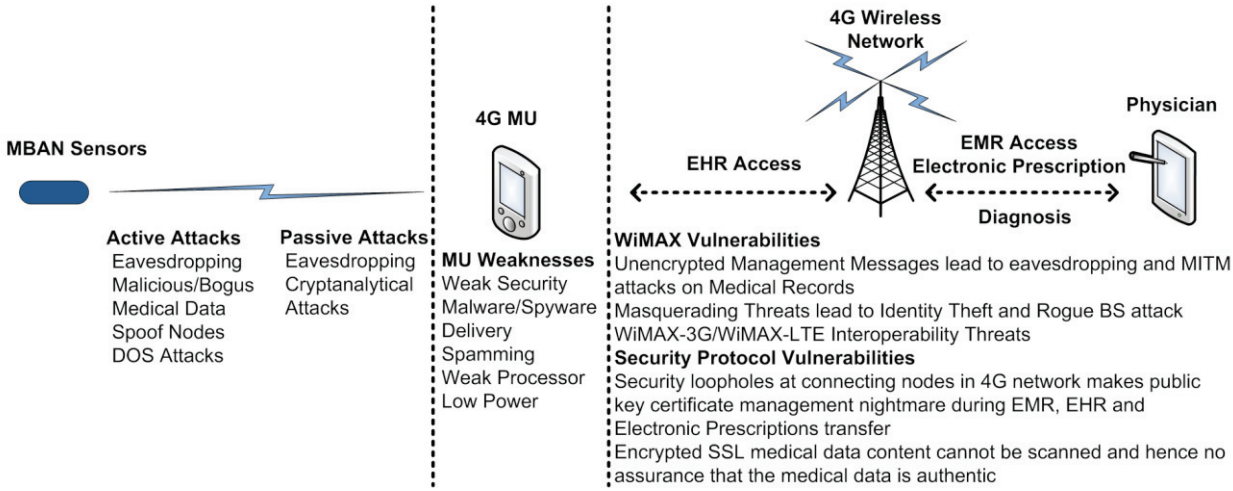

Fig. 2 Security Issues and Vulnerabilities of Health Records in 4G Network

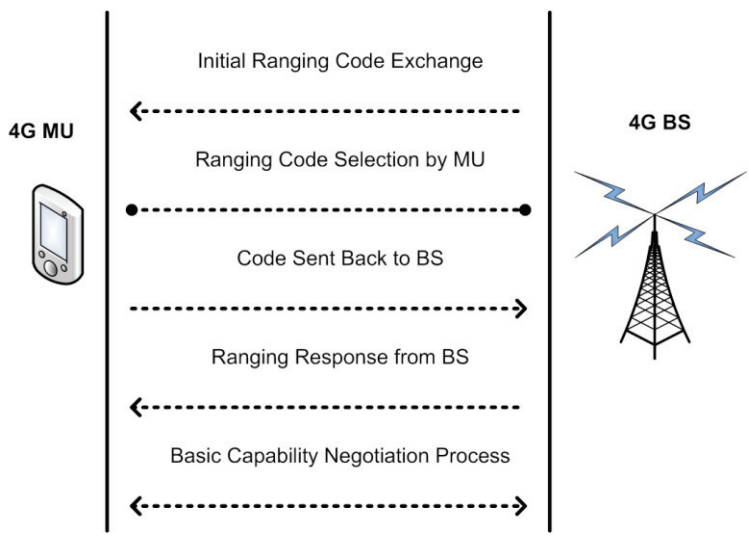

Fig. 3 Initial Network Entry Procedure by a Mobile Unit

3.2 Security issues associated with health records in WiMAX 4G network

Security issues in WiMAX involve vulnerabilities in Data Link (DL) layer and connection based security protocols, authentication threats, and weak security mechanisms in 4G devices. We discuss them in the subsections below.

3.2.1 Vulnerabilities of WiMAX in the Data Link layer

Mobile WiMAX has vital security flaws in the MAC sub layer. The initial network entry procedure is very important since it is the first step to establish a connection in Mobile WiMAX. It is performed by taking several

steps such as (a) initial Ranging process, (b) MU Basic Capability negotiation, (c) Privacy Key Management (PKM) authentication and (d) registration process. The initial network entry procedure is shown in Fig. 3. In this procedure [5, 9], when a 4G MU enters the network to upload health data, it scans the downlink channel and synchronizes with it. In this downlink, the WiMAX base station (BS) announces the initial ranging code for the MU. One of these codes is selected by the MU. This is sent back to BS for initial ranging. The BS station then responds back by sending a Ranging-Response (RNG-RSP) message. The next step involves MU basic capability negotiation process. These steps are performed by initiating multiple management (request-response) messages. These management messages are unencrypted and hence the attacker can eavesdrop on these messages, modify them, and send them back to the MU or the BS. The attacker can also modify the RNG-RSP messages, set the connection status as failed and re send it back to the MU. The MU will see this as a failure to establish connection, and will go for the initial ranging process again. The attacker may continue this Man in the Middle (MITM) attack through modification of RNG-RSP messages leading to complete denial of services (DoS) to the MU.

3.2.2 Authentication Threats in WiMAX

Mobile WiMAX is vulnerable to masquerading threat in which an attacker assumes the identity of the legitimate MU. There are two techniques to perform this type of attack, (a) Identity theft and (b) Rogue BS attack. In identity thefts, an attacker reprograms a mobile device using the hardware address of a legitimate user. The address can be easily stolen by intercepting the management messages during initial network entry procedures. In a rogue BS attack the attacker sends messages to the MU and forces it to believe that it is connected to a BS. The attacker can then receive all the messages from the MU. This rogue BS attack is partially solved by replacing the older version of PKM protocol with a newer version but the system is still susceptible to attacks. These attacks are possible mostly in public environment like airport, malls, etc.

3.3 Vulnerabilities in Connection based Security Protocols

4G technologies (WIMAX, LTE) are All-IP based networks and hence healthcare businesses and applications may use standard connection based security protocols [7] like HTTPS, SSL (Secure Socket layer) and TLS (Transaction Layer Security). Health information acts in almost all countries require use of these security protocols. In USA, the Health Insurance Portability and Accountability Act (HIPAA) mention SSL to be a minimum requirement for all Internet-facing systems which manage electronic patient healthcare information (EPHI) in any form. Connection-based security protocols demand reliable communication and continuous network connectivity which cannot be guaranteed in mobile environment. The basic idea is to secure communication channels and hence, secure everything that passes through those channels. This approach has several problems. Direct connection between client and server must be established. If an application has multiple intermediaries to provide value-added services, multiple HTTPS connections must be piped together. That not only opens potential security holes at connecting nodes, but also makes public key certificate management extremely difficult. This problem may be severe in current scenario where users have intermediaries to either inter-operate between WiMAX and 3G or perform interworking between 4G technologies (WiMAX and LTE). EMR and EHR access over 4G networks may be seriously compromised. Electronic prescription systems using SSL and public key certificates will be extremely vulnerable. A major loophole in the SSL encrypted transmission is that the network proxies are not capable of scanning the encrypted SSL contents. Thus, the content is secure from eavesdropping but there is no way to assure that the content is not malicious. For sensitive medical data transmission like EMR, EHR and electronic prescriptions over 4G network, we must secure content rather than securing only channels.

3.4 Vulnerabilities in 4G Mobile Devices

The protocol stack in Mobile WiMAX is loaded with heavyweight and resource intensive algorithms that do not take into account the limitations of a mobile handheld device. Limitations in handheld and cell phone hardware can lead to new threats that are not present in PC and servers. Some of these are caused by a general lack of processing power associated with handheld mobile devices. An example of a security threat associated with limited processing

power is the decision to leave data in plaintext, rather than encrypting it. This can arise when the algorithm to perform some kinds of encryption is processor-intensive. A single encryption or decryption operation on a desktop might take only a few seconds, the same operation on a low-powered mobile device with a relatively weaker processor might take several minutes. Most cell phone and tablet users seldom employ security mechanisms built into a device and apply settings that can be easily determined or bypassed. Instant messaging and multimedia services supported on many phones are means of malware delivery. Unauthorized person may pretend to be a doctor and send text resulting in installation of malwares.

4. Context Aware Security Scheme for Health Records

The shortcomings mentioned in the traditional security technologies discussed above indicates that there is a need to enhance the security features of Mobile WiMAX to make it useful for transmission of health data. We argue that a security scheme which uses minimal user input and transparent to users is relatively more robust and less resource intensive. In our on-going work, we propose to use context information like Location Coordinates (Longitude - Lo and Latitude - La) of the mobile unit and time to develop a highly reliable security and authentication scheme. We create a secured identity called "Location Signature (LS)" for a user request. LS is a 2-tuple record consisting of Lo/La and time (T) of transaction. A LS record is created continuously in real time and added to a chain of LS records. This chain of LS records is used for security and authentication of the legitimate user.

4.1 Motivation for using Location Information as a Security Feature in Mobile WiMAX

We are the first to introduce the concept of LS for developing a security and authentication scheme [6]. Our motivation for using LS to develop a robust security and authentication mechanism is based on the following assertions:

- LS create a unique identity of a mobile user. This is based on the fact that the combined context information of location (Lo/La) and time is always unique for any user. This secured identity is the fundamental component of our scheme that is used to authenticate a legitimate user. For a malicious user, it is almost impossible to imitate this secured identity.
- It is extremely difficult, if not impossible, to hack LS.
- Location identity of a mobile device adds a new dimension to mobile WiMAX security. It can supplement or complement existing security mechanisms. The LS can be used as a security mechanism when other systems have been compromised because it will always be unique for a user at any point in time. We illustrate why it is extremely hard to forge Lo/La which is the core component of our LS scheme.

4.2 Why Lo/La cannot be easily forged?

The Global Positioning System (GPS) receiver of the mobile device receives Lo/La in the form of strings. The hardware interface for GPS units is designed to meet the National Marine Electronics Association (NMEA) requirements. This data includes PVT (position, velocity, time) computed by the GPS. The idea of NMEA strings is to send a line of data called a *Sentence* which is totally self contained and independent from other sentences. There are standard sentences for each device category and proprietary sentences can be defined for use by the individual company. A common NMEA Sentence used for location information is:

*$GPGGA,123519,4807.038,N,01131.000,E,1,08,0.9,545.4,M,46.9,M,,*47*

This sentence has other information including 4807.038, N = La 48 deg 07.038' N and 01131.000, E =Lo 11 deg 31.000' E. After receiving the strings from the satellite, Lo/La is parsed out and sent to a server for the required application to work. To access this location information in java based MUs, a java application called MIDlet has to be loaded into the mobile device. A MIDlet is downloaded from a web server by a process called Over the Air (OTA) provisioning. The MIDlet java archive (Jar) file which uses the standard Application Program Interfaces (APIs) are developed and provided by the industry leaders like Java Community Process (JCP), Qualcomm Inc., etc.

The Jar files are accessed by another java file called the Java Application Descriptor (Jad) file that contains all the information about the jar files of the MIDlet. To access jar files present in the web server, the Jad file has to be signed with a Digital Signature which is provided by the mobile service provider. Thus, only those mobile applications which are digitally signed and present in the mobile device may access Lo/La for further usage. This totally prevents unauthorized access to Lo/La. Similar security features to prevent access of location information is present in other mobile platforms like Android, Apple OS etc. As a result Lo/La cannot be forged by a malicious user. Future work in this research project includes development of algorithms to implement this scheme and evaluate it in a mobile broadband environment to transmit mobile health data.

5. Conclusion

MHM is one of most important applications that are being implemented using the upcoming mobile broadband networks like WiMAX and LTE. An important aspect of MHM is secured transfer of mobile health data or records. In this work, we have identified several security threats and vulnerabilities associated with the transmission of the EHR, EMR and physiological data that is collected using a MBAN. To address these threats, we have proposed a context aware authentication scheme that uses location and time information of the MU. In our future work, we aim to implement this scheme and evaluate its performance during health data/records transmission in mobile broadband environment.

References

1. R. S. H. Istepanian, E. Jovanov, and Y. T. Zhang, M-health: beyond seamless mobility for global wireless healthcare connectivity-Editorial, IEEE Trans. Inf. Technol. Biomed., 8, no. 4, pp. 405-414, Dec. 2004.
2. FCC Mobile Network Plan could revolutionize healthcare, http://www.computerworld.com/s/article/9174429/FCC_mobile_network_plan_ could_revolutionize_ health_care.
3. D. Acharya and V. Kumar, Mobile Broadband based Healthcare Management: Advantages, Issues and Challenges, Intl Journal for Comp in Healthcare, Vol. 1, no. 3, 2011.
4. D. Garets and M. Davis, Electronic Medical Records vs. Electronic Health Records: Yes, There is a Difference, HIMSS Analytics White Paper, 2006.
5. P. Rengaraju,C. Lung,Y. Qu and A. Srinivasan, Analysis on Mobile Wimax Security, IEEE Intl Conference on Sc and Tech for Humanity, 2009.
6. V. Kumar and D. Acharya, Web Bazaar. A Location-Dependent Secured Mobile Web Service System, Ingénierie des Systèmes d'Information, Networking and Information Systems,Volume 10, no. 5, pp. 123-145, 2005.
7. M.Yuan, Enterprise J2ME: Developing Mobile Java Applications, Prentice Hall, 2003.
8. IEEE 802.16-2005, IEEE Standard for Local and Metropolitan Area Netwoks, - Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems, IEEE Press, 2005.
9. T. Han et. al, Analysis of Mobile WiMAX Security: Vulnerabilities and Solutions, Proc. Of 5th Intl Conf. On Mob Adhoc and Sensor Syst., 2008.
10. 3GPP – LTE, http://www.3gpp.org/LTE